PTO/SB/17p (11-04)

PETITION FEE
Under 37 CFR 1.17(f), (g) & (h)
TRANSMITTAL

(Fees are subject to annual revision)

Send completed form to: Commissioner for Patents
P.O. Box 1450, Alexandria, VA 22313-1450

Application Number	10/791,452
Filing Date	March 1, 2004
First Named Inventor	FURUKAWA, Hiroshi
Art Unit	2180
Examiner Name	Unassigned
Attorney Docket Number	16869Y-108700US

Enclosed is a petition filed under 37 CFR §1.102(d) that requires a processing fee (37 CFR 1.17(f), (g), or (h)). Payment of $ 130.00 is enclosed.

This form should be included with the above-mentioned petition and faxed or mailed to the Office using the appropriate Mail Stop (e.g., Mail Stop Petition), if applicable. *For transmittal of processing fees under 37 CFR 1.17(i), see or PTO/SB/17i.*

Payment of Fees (small entity amounts are NOT available for the petition fees)

☒ The Commissioner is hereby authorized to charge the following fees to Deposit Account No. 20-1430 :

☒ petition fee under 37 CFR 1.17(f), (g) or (h) ☒ any deficiency of fees and credit of any overpayments

Enclose a duplicative copy of this form for fee processing.

☐ Check in the amount of $_____ is enclosed.

☐ Payment by credit card (Form PTO-2038 or equivalent enclosed). Do not provide credit card information on this form.

Petition Fees under 37 CFR 1.17(f): Fee $400 Fee Code 1462

For petitions filed under:

§ 1.53(e) - to accord a filing date.
§ 1.57(a) - to accord a filing date.
§ 1.182 - for decision on a question not specifically provided for.
§ 1.183 - to suspend the rules.
§ 1.378(e) - for reconsideration of decision on petition refusing to accept delayed payment of maintenance fee in an expired patent.
§ 1.741(b) - to accord a filing date to an application under § 1.740 for extension of a patent term.

Petition Fees under 37 CFR 1.17(g): Fee $200 Fee Code 1463

For petitions filed under:

§ 1.12 - for access to an assignment record.
§ 1.14 - for access to an application.
§ 1.47 - for filing by other than all the inventors or a person not the inventor.
§ 1.59 - for expungement of information.
§ 1.103(a) - to suspend action in an application.
§ 1.136(b) - for review of a request for extension of time when the provisions of section 1.136(a) are not available.
§ 1.295 - for review of refusal to publish a statutory invention registration.
§ 1.296 - to withdraw a request for publication of a statutory invention registration filed on or after the date the notice of intent to publish issued.
§ 1.377 - for review of decision refusing to accept and record payment of a maintenance fee filed prior to expiration of a patent.
§ 1.550(c) - for patent owner requests for extension of time in ex parte reexamination proceedings.
§ 1.956 - for patent owner requests for extension of time in inter partes reexamination proceedings.
§ 5.12 - for expedited handling of a foreign filing license.
§ 5.15 - for changing the scope of a license.
§ 5.25 - for retroactive license.

Petition Fees under 37 CFR 1.17(h): Fee $130 Fee Code 1464

For petitions filed under:

§ 1.19(g) - to request documents in a form other than that provided in this part.
§ 1.84 - for accepting color drawings or photographs.
§ 1.91 - for entry of a model or exhibit.
✓ **§ 1.102(d)** - to make an application special.
§ 1.138(c) - to expressly abandon an application to avoid publication.
§ 1.313 - to withdraw an application from issue.
§ 1.314 - to defer issuance of a patent.

Signature	February 7, 2006 (Date)
Chun-Pok Leung (Typed or printed name)	41,405 (Registration No., if applicable)

PATENT
Attorney Docket No.: 16869Y-108700US
Client Ref. No.: HT188401

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

HIROSHI FURUKAWA *et al.*

Application No.: 10/791,452

Filed: March 1, 2004

For: STORAGE SUBSYSTEM, STORAGE SYSTEM, AND COMMUNICATION CONTROL METHOD

Customer No.: 20350

Examiner: Unassigned

Technology Center/Art Unit: 2180

Confirmation No.: 3451

PETITION TO MAKE SPECIAL FOR NEW APPLICATION UNDER M.P.E.P. § 708.02, VIII & 37 C.F.R. § 1.102(d)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is a petition to make special the above-identified application under MPEP § 708.02, VIII & 37 C.F.R. § 1.102(d). The application has not received any examination by an Examiner.

(a) The Commissioner is authorized to charge the petition fee of $130 under 37 C.F.R. § 1.17(i) and any other fees associated with this paper to Deposit Account 20-1430.

(b) All the claims are believed to be directed to a single invention. If the Office determines that all the claims presented are not obviously directed to a single invention, then Applicants will make an election without traverse as a prerequisite to the grant of special status.

(c) Pre-examination searches were made of U.S. issued patents, including a classification search and a computer database search. The searches were performed on or around September 9, 2004, and were conducted by a professional search firm, Kramer & Amado, P.C. The classification search covered Class 711 (subclasses 151, 161, and 163) and Class 713 (subclasses 193 and 202) for the U.S. and foreign subclasses identified above. The computer database search was conducted on the USPTO systems EAST and WEST. The inventors further provided two references considered most closely related to the subject matter of the present application (see references #5-6 below), which were cited in the Information Disclosure Statements filed on March 1, 2004.

(d) The following references, copies of which are attached herewith, are deemed most closely related to the subject matter encompassed by the claims:

(1) U.S. Patent No. 4,413,328;

(2) U.S. Patent No. 4,947,318;

(3) U.S. Patent No. 6,728,844 B2;

(4) U.S. Patent No. 6,779,083 B2;

(5) European Patent Publication No. EP 1,117,028 A2; and

(6) Japanese Patent Publication No. JP 2001-265655.

(e) Set forth below is a detailed discussion of references which points out with particularity how the claimed subject matter is distinguishable over the references.

A. Claimed Embodiments of the Present Invention

The claimed embodiments relate to communication between a host computer and a storage subsystem and, more particularly, to a filtering technology and a communication cut off technology in communication at the time of an access from the host computer to a logical unit in the storage subsystem.

Independent claim 1 recites a storage subsystem which is connected to a host computer through a communication line. The storage subsystem comprises an interface which is used for connecting to the communication line, wherein the interface comprises a

first filter which judges, on the occasion of having received communication packets from the communication line, whether there is a communication packet with a predetermined format for use in an access to the storage subsystem, among the communication packets. The interface further comprises a traffic measuring and judging unit which measures traffic of all communication packets received in the interface, and traffic of a communication packet judged not to be the packet with the format in the first filter, respectively, and by using the both traffics, judges whether a communication failure is generated or not, and a communication failure alerting unit which alerts a management server connected to the storage subsystem and comprises a function of displaying information alerted, in case that it is judged that a communication failure is generated in the traffic measuring and judging unit.

Independent claim 9 recites a computer readable storage medium including a program for a computer mounted on a storage subsystem connected to a host computer through a communication line. The program comprises code for connecting to the communication line; code for judging, on the occasion of having received communication packets from the communication line through connecting to the communication line, whether there is a communication packet with a predetermined format for use in an access to the storage subsystem, among the communication packets; code for receiving the communication packet judged to be for the access in the judging, and judges whether it is a communication packet permitted to access to a storage area in the storage subsystem and transmitted from the host computer or not; code for measuring traffic of all communication packets received in connecting to the communication line, and traffic of a communication packet judged not to be the packet with the format in the first filter, respectively, and by using the both traffics, judging whether a communication failure is generated or not; and code for alerting a management server connected to the storage subsystem and displaying information alerted, in case that it is judged that a communication failure is generated in measuring the traffic of all communications packets received in connecting to the communication line.

Independent claim 12 recites a computer readable storage medium including a program for a computer mounted on a management server which is connected to a storage subsystem. The program comprises code for referring to the traffic log, in case that it is alerted from a communication failure alerting unit of the storage subsystem that a communication failure is generated, and searching a source of the communication packet which causes the communication failure.

Independent claim 13 recites a computer readable storage medium including a program for a computer mounted on a management server which is connected to a storage subsystem. The program comprises code for referring to the traffic log, in case that it was alerted from a communication failure alerting unit of the storage subsystem that a communication failure is generated, and searching a source of the communication packet which causes the communication failure, and code for controlling, based on information of a source searched in the searching, a relay device which relays communication to the storage subsystem disposed on the communication line for receiving a communication packet so as to cut off communication from the source.

Independent claim 15 recites a storage system in which a storage subsystem, a host computer, and a management server are connected by a communication line. The storage subsystem comprises an interface which connects to the communication line. The interface comprises, a first filter which judges, on the occasion of having received communication packets from the communication line, whether there is a communication packet with a predetermined format for use in an access to the storage subsystem, among the communication packets, a second filter which receives the communication packet judged to be for the access in the first filter, and judges whether it is a communication packet permitted to access to a storage area in the storage subsystem and transmitted from the host computer or not, a traffic measuring and judging unit which measures traffic of all communication packets received in the interface, and traffic of a communication packet judged not to be the packet with the format, respectively, and by using the both traffics, judges whether a communication failure is generated or not, a communication failure alerting unit which alerts the management server, in case that it is judged that a communication failure is generated in the traffic measuring and judging unit, and a traffic log recording unit which records, as a traffic log, communication information of a communication packet judged not to be the communication packet with the format in the first filter and a communication packet judged not to be the communication packet transmitted from the host computer permitted to access in the second filter. The management server comprises a display device which displays the alert received from the communication failure alerting unit, an improper communication source analyzing unit which refers to the traffic log, in case that it is alerted from a communication failure alerting unit of the storage subsystem that a communication failure is generated, and searches a source of the communication packet which causes the communication failure, and a relay

device control unit which controls, based on information of a source searched in the improper communication source analyzing unit, a relay device which relays communication to the storage subsystem disposed on the communication line so as to cut off communication from the source.

One of the benefits that may be derived is that it is possible to heighten security in a storage subsystem connected to a communication line, and to secure a network QoS to a storage subsystem.

B. Discussion of the References

1. U.S. Patent No. 4,413,328

This reference relates to a storage subsystem that employs removable media with a display at each recorder, and controls the display in such a manner as to enhance subsystem operation by reducing operator error and increase data and subsystem security. See column 1, lines 60-65. For instance, section 24 relates to certain characters to be displayed in display 28 relating to error conditions detected in storage unit (SU) 13. Message control logic module or program 63 is operatively associated with a message table 64, which is a table look-up mechanism for converting SU 13 generated status and error message to a display code for human comprehension.

The reference is directed to using and controlling display information relating to error conditions in order to enhance subsystem. It does not disclose judging whether a communication failure is generated or not, alerting of a communication failure, or searching for a source of the communication packet that causes the communication failure. More specifically, the reference fails to teach measuring traffic of all communication packets received in connecting to the communication line, and traffic of a communication packet judged not to be the packet with the format in the first filter, respectively, and by using the both traffics, judging whether a communication failure is generated or not; and alerting a management server connected to the storage subsystem and displaying information alerted, in case that it is judged that a communication failure is generated in measuring the traffic of all communications packets received in connecting to the communication line (as recited in independent claims 1, 9, and 15); and referring to the traffic log, in case of a communication

failure, and searching a source of the communication packet which causes the communication failure (as recited in independent claims 12 and 13).

2. U.S. Patent No. 4,947,318

This reference discloses that when the storage volume is loaded into a storage unit, the data protection information stored in the storage volume is automatically read out of the storage volume and stored in a memory of the storage unit by the internal control unit of the storage unit, and the data protection information stored in the memory is correlated with an access request for data in the storage volume to check the validity of the data access so that the specified data in the storage volume is protected from an invalid or unjust access without the aid of host computer or operation by the operator. For instance, when the host computer 1 issues a read instruction to a protection area of the magnetic disk volume 4, the protection area access decision controller 25 correlates the password sent from the host computer 1 with the password stored in the internal memory 23 in step 507. If the passwords are equal, the program proceeds to the step 503, but if they are unequal, the controller 25 sends an access reject (inhibit) signal to the host computer 1 via the control line 102 in step 509 to reject the accessing. If the host computer 1 issues a write instruction to the protection area, the protection area access decision controller 25 checks to see if the flag in the corresponding protection area defining information in the internal memory 23 indicates write protection in step 508. If the flag does not indicate write protection, the program proceeds to the step 503, but if it indicates write protection, the controller 25 sends a write reject signal to the host computer 1 in step 509.

The reference relates to the use of protection key information to permit or inhibit access to storage. It does not disclose judging whether a communication failure is generated or not, alerting of a communication failure, or searching for a source of the communication packet that causes the communication failure. More specifically, the reference fails to teach measuring traffic of all communication packets received in connecting to the communication line, and traffic of a communication packet judged not to be the packet with the format in the first filter, respectively, and by using the both traffics, judging whether a communication failure is generated or not; and alerting a management server connected to the storage subsystem and displaying information alerted, in case that it is judged that a communication failure is generated in measuring the traffic of all communications packets

received in connecting to the communication line (as recited in independent claims 1, 9, and 15); and referring to the traffic log, in case of a communication failure, and searching a source of the communication packet which causes the communication failure (as recited in independent claims 12 and 13).

3. U.S. Patent No. 6,728,844 B2

This reference discloses a standardized fiber channel as an interface between one or more host computers and a storage control device. It also includes host computers and a storage control device plus more than one storage device operable under control of the storage control device, wherein the fiber channel connection storage control device has a security function in the environment capable of physically receiving any access from the host computers, and eliminating or deterring unauthorized access attempts from the host computers to the storage control device, which did not have any means for rejecting unauthorized access from host computers. See column 2, lines 10–20. By causing the storage controller 40 to manage the one-to-one correspondence of those ports of the host computers and the storage controller using the log-in request control table 130, in the way as described in steps S71 to S75 of Fig. 7, it is possible for users to prevent any unauthorized access attempts from host computers on a port-by-port basis thereby maintaining enhanced security.

The reference provides a security function for eliminating or deterring unauthorized access attempts to the storage. It does not disclose judging whether a communication failure is generated or not, alerting of a communication failure, or searching for a source of the communication packet that causes the communication failure. More specifically, the reference fails to teach measuring traffic of all communication packets received in connecting to the communication line, and traffic of a communication packet judged not to be the packet with the format in the first filter, respectively, and by using the both traffics, judging whether a communication failure is generated or not; and alerting a management server connected to the storage subsystem and displaying information alerted, in case that it is judged that a communication failure is generated in measuring the traffic of all communications packets received in connecting to the communication line (as recited in independent claims 1, 9, and 15); and referring to the traffic log, in case of a communication

failure, and searching a source of the communication packet which causes the communication failure (as recited in independent claims 12 and 13).

4. U.S. Patent No. 6,779,083 B2

This reference discloses that in this storage subsystem, a user can make setting of accessible LUN and setting on a connection interface in an arbitrary group unit of computers under a single port without changing existing processing, limitation and other functions of the computers. Therefore, this storage subsystem can accomplish an access control function, that is, a LUN security function, for computer groups having a plurality of kinds of OS under a single port. In one example, the host computer of WWN1125 and the host computer 1126 are categorized as Group F 1110 having an OS kind 7 that can recognize only 256 LU under the single port. It will be assumed that a user's request for recognizing 512 LU under the single port exists in practice. In this case, the host computer of WWN1125 and the host computer 1126 are again registered as a separate Group G 1111. Since both host computers can recognize maximum 256 LU, LU0 to 255 for Group F 1110 and LU0 to 255 for Group G 1111 are defined as access permitted LU. The storage areas #0 to 255 are allocated to LU0 to 255 of Group F 1110 and the storage areas #256 to 512 are allocated to LU0 to 255 of Group G 1111. In this way, 512 LU are given without changing the existing processing, limitation and other functions of the host computers, and the LUN security function of the invention is accomplished. See col. 11, lines 30-45.

The reference relates to providing an access control function under a single port without changing existing processing, limitation and other functions of the computers. It does not disclose judging whether a communication failure is generated or not, alerting of a communication failure, or searching for a source of the communication packet that causes the communication failure. More specifically, the reference fails to teach measuring traffic of all communication packets received in connecting to the communication line, and traffic of a communication packet judged not to be the packet with the format in the first filter, respectively, and by using the both traffics, judging whether a communication failure is generated or not; and alerting a management server connected to the storage subsystem and displaying information alerted, in case that it is judged that a communication failure is generated in measuring the traffic of all communications packets received in connecting to the communication line (as recited in independent claims 1, 9, and 15); and referring to the

traffic log, in case of a communication failure, and searching a source of the communication packet which causes the communication failure (as recited in independent claims 12 and 13).

5. European Patent Publication No. EP 1,117,028 A2

This reference relates to techniques for performing security functions in computer storage subsystems in order to prevent illegal access by the host computers according to logical unit (LU) identity. Management tables can be used to disclose the Logical Unit in the storage subsystem to the host computers in accordance with the user's operational needs. In a specific embodiment, accessibility to a storage subsystem resource can be decided when an Inquiry Command is received, providing systems and apparatus wherein there is no further need to repeatedly determine accessibility for subsequent accesses to the Logical Unit. As shown in Figure 8, the user creates an "LUN Access Management Table" in step 801. Each host computer initiates a LOGIN procedure to the storage subsystem in step 802. The storage subsystem receives a frame which contains the Inquiry Command transferred by the host computer to get the status of the Logical Unit in the storage subsystem in step 803. The storage subsystem searches the "LUN Access Management Table" using the WWN obtained as a key in step 804. In step 805, the storage subsystem makes a determination whether the Virtual LUN corresponding to the WWN is actually obtained in step 804.

The reference is directed to the use of an "LUN Access Management Table" to perform security functions in computer storage subsystems. It does not disclose judging whether a communication failure is generated or not, alerting of a communication failure, or searching for a source of the communication packet that causes the communication failure. More specifically, the reference fails to teach measuring traffic of all communication packets received in connecting to the communication line, and traffic of a communication packet judged not to be the packet with the format in the first filter, respectively, and by using the both traffics, judging whether a communication failure is generated or not; and alerting a management server connected to the storage subsystem and displaying information alerted, in case that it is judged that a communication failure is generated in measuring the traffic of all communications packets received in connecting to the communication line (as recited in independent claims 1, 9, and 15); and referring to the traffic log, in case of a communication

failure, and searching a source of the communication packet which causes the communication failure (as recited in independent claims 12 and 13).

6. Japanese Patent Publication No. JP 2001-265655

This reference discloses a technique to provide a security function in a storage subsystem using the flexible and efficient presentation method of storage resources by performing execution with high-speed judgment logic without affecting a processing on the side of a host computer. An information WWN for uniquely identifying the host computer, a management table where the correspondence of a logical unit number LUN inside the storage subsystem for which access is permitted to the host computer and a virtual LUN for presenting the LUN to be the access object to the host computer by a user optional method is described and the management table where the correspondence of the WWN and a dynamically allocated management number S-ID is described are stored in a nonvolatile memory inside the storage subsystem beforehand.

As discussed in the present application at page 1, line 22 to page 3, line 5, the storage system as disclosed in the reference comprises, on a nonvolatile memory in a storage subsystem, in addition to a LUN access management table which manages a WWN (World Wide Name) as information which uniquely identifies a host computer, a LUN (logical Unit Number) as a number of a logical unit in a storage subsystem which permitted an access from the host computer, and a virtual LUN as a number of a virtual LU that a user or an operating system on the host computer arbitrarily assigned in parallel with the LUN, by associating them one another. In such communication that the host computer accesses to the storage subsystem, the storage system further comprises a WWN-S-ID management table which manages a S-ID (Source ID) as a management number which is dynamically assigned at the time of log-in and which is always constant during the host computer is in operation, and the WWN of the host computer, by associating them each other.

In the storage system, with reference to these two management tables, right and wrong of an access to a logical unit is judged at the time point of generation of an inquiry command at the time of log-in. After that, there is no necessity to repeat this judgment. On this account, it is possible to limit right and wrong of an access with each of a logical unit, over maintaining and operating a storage subsystem with high performance, which realizes strong security. In this regard, however, the storage system disclosed in the reference is a

system which was built up by a dedicated network, such as a SAN (Storage Area Network) in which a host computer and a storage subsystem are connected to be networked by using a dedicated interface called as Fiber Channel (FC). Therefore, it is a premise that only a SCSI command, which is a command set for an access from a host computer to a storage subsystem, is transmitted to a storage subsystem.

The reference does not disclose judging whether a communication failure is generated or not, alerting of a communication failure, or searching for a source of the communication packet that causes the communication failure. More specifically, the reference fails to teach measuring traffic of all communication packets received in connecting to the communication line, and traffic of a communication packet judged not to be the packet with the format in the first filter, respectively, and by using the both traffics, judging whether a communication failure is generated or not; and alerting a management server connected to the storage subsystem and displaying information alerted, in case that it is judged that a communication failure is generated in measuring the traffic of all communications packets received in connecting to the communication line (as recited in independent claims 1, 9, and 15); and referring to the traffic log, in case of a communication failure, and searching a source of the communication packet which causes the communication failure (as recited in independent claims 12 and 13).

(f) In view of this petition, the Examiner is respectfully requested to issue a first Office Action at an early date.

Respectfully submitted,

Chun-Pok Leung
Reg. No. 41,405

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, 8th Floor
San Francisco, California 94111-3834
Tel: 650-326-2400
Fax: 415-576-0300
Attachments
RL:rl
60409020 v1